OPEN ACCESS

International Journal Of Modern Engineering Research (IJMER)

A Study on Security Mechanisms and Issues in Cloud Architecture Frame work

VenkateswarluManinti , Dr. NageshwarPulipati

Abstract:*Cloud computing is an innovation of existing technology which provides long-dreamed vision of computing as utility. The emergence of this novel technology in IT business has decoyed most of organizations in both private and public sector. Although cloud introduces the innovative and cost effective concept of on demand service, pay as you go, and resource allocation, security is often the area of concern in terms of its adoption. The existing security-based solutions for cloud-based platform are either based on single tamper-proof hardware or homomorphic encryption. Hardware-based solution lacks scalability, while homomorphic encryptions are only a theory. Moreover, traditional defense in-depth security mechanism cannot be directly implemented in cloud-based platform due to the varying nature of its service and deployment model. However, the same concept of multi-layered security mechanism can be proposed to secure the cloud-based platform.*

Keywords:*Cloud Computing; Security Mechanisms; Security Issues; Cloud Architecture Framework*

I. INTRODUCTION

Cloud computing is the evolution of an existing IT infrastructure that provides a long-dreamed vision of computing as a utility. The emergence of cloud technologies over last several years had significant impacts on many aspects of IT business. According to the survey conducted about cloud computing, most of medium and small companies use cloud computing services due to various reasons, which include reduction of cost in infrastructure and fast access to their application. Cloud computing has been described in terms of its delivery and deployment models. Although cloud computing emerges from existing technologies.

II. LITERATURE REVIEW

Cloud Architecture -Service, Deployment models and Characteristics

The importance of cloud computing and its adoption can be best described in terms of its underlying characteristics, delivery and deployment models, how customers can use these services, and how to provide them securely.

Cloud computing consists of FIVE characteristics,THREE service models and FOUR deployment models. These models and characteristics lie on the top of each other, thereby forming a stack of a cloud. Below Fig.1 represents the logical construction of cloud computing.

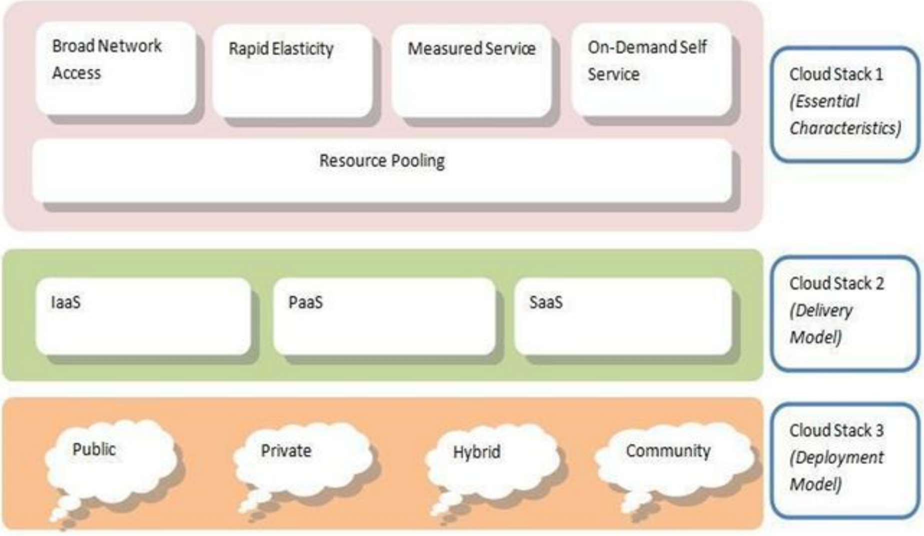


Fig.1 Cloud Architecture

The FIVE characteristics of each cloud are: location-independent resource pooling, on-demand self-service, rapid/instant elasticity, broad/transparent network access, and measured/regular service.

❖ These FIVE characteristics are located at the top of cloud stack.

The THREE service models of cloud computing environment are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

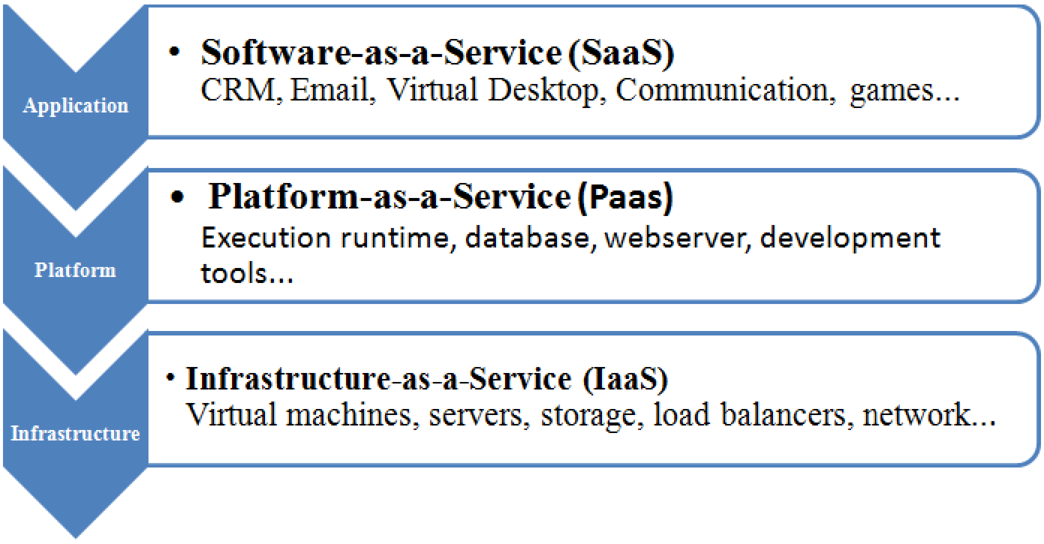

Application
• Software-as-a-Service (SaaS)
CRM, Email, Virtual Desktop, Communication, games…
Platform
• Platform-as-a-Service (Paas)
Execution runtime, database, webserver, development tools…
Infrastructure
• Infrastructure-as-a-Service (IaaS)
Virtual machines, servers, storage, load balancers, network…

Fig.2 Cloud Computing Environment

Software as a service (SaaS)

The software-as-a-service (SaaS) service-model involves the cloud provider installing and maintaining software in the cloud and users running the software from their cloud clients over the Internet (or Intranet). The users' client machines require no installation of any application-specific software - cloud applications run on the server (in the cloud). SaaS is scalable, and system administration may load the applications on several servers. In the past, each customer would purchase and load their own copy of the application to each of their own servers, but with the SaaS the customer can access the application without installing the software locally. SaaS typically involves a monthly or annual fee.

SaaS is built on the top of PaaS which provides delivery of business applications designed for a specific purpose. SaaS comes in two distinct modes named simple multi-tenancy and fine grained multi-tenancy. An example of SaaS is the SalesForce.com CRM application.

Platform as a service (PaaS)

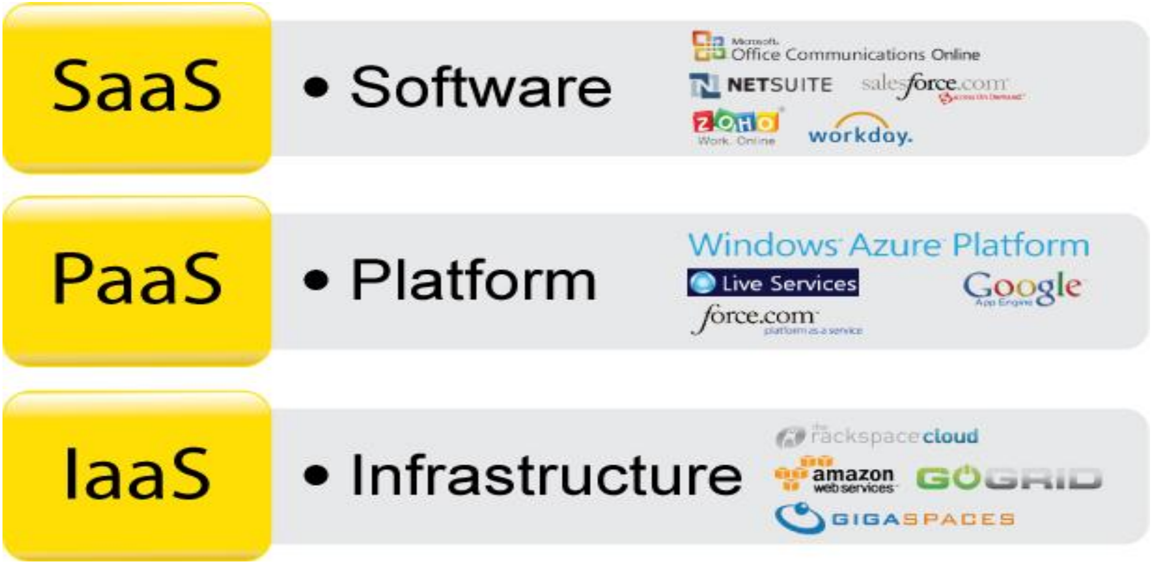
Platform as a service is cloud computing service which provides the users with application platforms and databases as a service. This is equivalent to middleware in the traditional (non-cloud computing) delivery of application platforms and databases.

PaaS is built on the top of IaaS, from where end-users can run their custom applications using their service providers' resources. Examples of PaaS are App Fog, Google App etc.

Infrastructure as a service (IaaS)

Infrastructure as a service is taking the physical hardware and going completely virtual (e.g. all servers, networks, storage, and system management all existing in the cloud). This is the equivalent to infrastructure and hardware in the traditional (non-cloud computing) method running in the cloud. In other words, businesses pay a fee (monthly or annually) to run virtual servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level.

Infrastructure-as-a-Service can be defined as virtual machines on demand, where users benefit from networking infrastructure facilities, computing services, and data storage. Amazon and Rackspace are leading vendors for IaaS platforms.



❖ These THREE services models reside at the second layer of cloud stack.

TheFOUR delivery modelsare,Public cloud, Private cloud, Community cloud, and Hybrid cloud.

- Public clouds are predominantly owned by large scale organizations and services owned by this cloud are made available to the general public or a broad industry group.
- Private cloud is owned solely by one organization and is available for a particular group.
- Community cloud is shared and managed by the particular organization and supported by the specific community that has shared concern.
- Hybrid cloud is composed of two or more clouds (private, public, and community)

.

❖ These FOUR deployment models reside at the third layer of a cloud stack.

Security Mechanisms and issues in Cloud Computing Platform

Cloud computing (delivery and deployment) models and characteristics raise new security challenges due to some incompatibility issues with existing security solutions.

Security mechanisms in cloud computing platforms followed by security mechanisms that are available and can be deployed in various cloud computing platforms. Security mechanisms in cloud computing platforms based on their delivery and deployment models followed by available security products and modules.

Security Overview

Cloud computing is a paradigm shift of technology that have emerged and has been adopted by many IT organizations in the recent year. This shift in technology has changed the overall architecture and system requirements, compared to traditional server-based systems. Cloud-based system architecture provides Internet-based services, computing and storage in all fields including health care, finance, government etc. with the reduced price. Therefore, it is more likely to be adopted by most of the IT organizations. While there is a serious concern for an organization to move towards the cloud based service, security risk associated within the platform are one of the urgent concern for an organization to make this move.

Different cloud based deployment models have brought the wide range of security risks and concerns that have to be evaluated and mitigated. Traditional defense in depth security model which include physical security, perimeter security, firewall, antivirus software, etc. are not directly applicable to cloud-based systems. This means that various organizations must adopt the best security practices and standards that are somehow incompatible to traditional defense in depth security models.However, the same principle of multi-layered security is still applicable.

In cloud-based platforms, no matter what we choose as our deployment model, we will be working with abstracted and virtualized environment. This means that software or platform will run on the top of shared physical infrastructure, which is managed either internally (in case of private cloud) or by CSP (in case of public cloud). This means the security architecture for application services will need to shift from platform to the application layer. For example, if application provided by the cloud vendor is Software as a Service, then the end-user have no control over the software development platform or infrastructure used and thus all the security countermeasures are needed to be placed at the application level.

Security Mechanisms for the Cloud Service Model

Cloud-based system addresses three service models named IaaS, PaaS. SaaS. These service models lie on the top of each other, thereby forming the stack of a cloud. The IaaS service model can be deployed using one of the deployment models, as discussed on Chapter 1. Hence security implications need to take into account considering both service and deployment models.

Security Mechanism for IaaS

Infrastructure-as-a-Service, sometimes also referred as utility computing, can be viewed as virtual machine on demand, where this virtual machine can be accessed remotely and made available on elastic basis. This means that all the necessary infrastructure, hardware, memory, networks and storage are provided by IaaS service model. Most of the security concerns for IaaS delivery model are due to sharing and pooling of resources, virtualized data center, and virtualization of hardware, resources and networks. No matter what we opt to choose as our deployment model for IaaS, security requirements for IaaS service model must be implemented at the level of host, virtual machine, network, storage, compute and memory.

For public/hybrid cloud model, all the cloud services are provided to cloud service clients via Internet. The cloud service client in this case may be client computer or any on-premises system that is connected to cloud-based IaaS system. Depending on the services offered by cloud-based IaaS system, we can control security state of the client system connected to cloud services. This can be done by enforcing the baseline security level of all clients to assure that the client has sufficient security tools, like anti-virus, anti-malware and up-to-date security patches. However, if these cloud services are available to an unaffiliated user, there is nothing that IaaS vendor can do to enforce security policy of this non-affiliated client. Therefore, system must be designed to support the level of network encryption or even in the worst scenario secure session must be established for the logging process.

Another issue associated within this delivery model is network availability. Attacks like DNS misdirection, Prefix hijacking, or distributed denial of service can seriously deteriorate the network availability of the system. Therefore, constant network monitoring and auditing tool must be implemented to mitigate the attacks on network availability. Moreover, in a private/hybrid cloud network resources are consumed form a common resource pool. Consequently, logical isolation of internal system is equally important for cloud-based IaaS system. This means that in order to secure the network system of our cloud-based IaaS delivery model virtual firewall, VLAN, virtual layer 2,3 switches, and IPSec isolation are needed to be considered and implemented.

Another issue associated with IaaS delivery model is due to its architectural representation of its cloud-based storage system. Cloud based storage system is designed for creating the pool of resources, abstracting the details like storage location, storage type, persistence of storage, etc. from its consumers. This means that data from multiple tenants reside on same disk or array and any breach in the system could lead to the exposure of private and sensitive data to a malicious user or unintended tenants. An appropriate access control (XACML) and authentication (SAML, Open ID) mechanisms in terms of identity of the user can mitigate this issue. The implementation details of this access control and authentication mechanisms depend on the deployment models of cloud-based platforms.

Public cloud, offering IaaS delivery model, may use web services through web portals to provide access control and authentication mechanisms. Hybrid cloud may use public cloud storage gateway appliance on premises, where the cloud storage API is translated into conventional data retrieval protocol, like ISCSI, NFS (Network File System), SMB (Server Messaging Block), etc.

Security Mechanism for PaaS

Platform-as-a-Service model is built on the top of IaaS, which provides complete development environment where application developers can create and deploy their applications. In contrast to traditional software development tools, like Visual Studio, PaaS offers a shared development environment. This means that there must be a mechanism within the system to ensure that customers are kept separate from each other. An appropriate authentication, access control and authorization mechanisms will ensure isolation of customers. A strong and implicit authentication mechanism ensures that user is correctly identified. Most of the Paas providers still rely on the same traditional user-name and password-based authentication and then apply access control and authorization mechanisms based on verification of the credentials provided. An alternative to this, two factor authentication mechanisms, like smart cards and biometrics, can be implemented. Moreover, identities-based authentication in terms of web services or SAML- based identity provider can be taken into account, where authentication authorization and access control in a PaaS system can be externalized.

Security Mechanism for SaaS

Software-as-a-Service is built on the top of PaaS, and all of the security mechanisms are implemented at an application level, regardless of its deployment model. Network security is typically not considered in the SaaS delivery model. However, it can be implemented with regards to some application specific control of SaaS solution. In a Public cloud scenario, high degree of trust in the cloud vendor is required, as the infrastructure and platform are under the supervision of cloud vendors. Therefore, security responsibility of both cloud vendor and customer are defined in the Service Level Agreement (SLA). Another factor to be considered for a SaaS-based solution is its APP's store. Cloud vendor may offer their application only from their app store, and there is a possibility that any malicious user can post malware in the app store. Google Android had a similar problem in the past. Moreover, one must also assume that SaaS-based software solution will be scanned by the hacker in order to identify the vulnerabilities before deploying it. Due to the absence of App's store in a private cloud, threats associated with malicious malware from outside of the company are no more the area of concern. However, App's developed with poor piece of code can be as detrimental as malware. This means that regardless of deployment model on a cloud-based platform, security guidelines for developing software based solutions, like SDL (Security Development Lifecycle), should be followed before developing SaaS-based solution in a cloud.

In this paper we will discuss security issues for cloud computing platforms provided by non-profit organizations that consist of industry representatives - Cloud Security Alliance (CSA) followed by two esteemed government organization, named National Institute of Standard and Technology (NIST) and European Network and Information Security Agency (ENISA).

III. SECURITY ISSUES IDENTIFIED CSA, NIST, ENISA

Security Issues identified by Cloud Security Alliance (CSA)

Cloud Security Alliance is a non-profit organization, initiated by industry representatives in November 2008 and later supported by large number of IT companies, including Google, VMware, Microsoft, IBM, Ericsson, etc. The main motive of this organization is to provide security assurance and education in the field of cloud computing.

CSA published its first draft “Security Guidance for Critical Area Focus In Cloud Computing” on April 2009 which provides information about security issue in cloud computing platforms. For our analysis, we use the current version (v3) of this draft. The guidance is divided into fourteen domains. The first domain named “Architectural Framework” gives brief information about cloud computing platform and its reference model from the security perspective. The rest of the domains are divided into top two categories named governance and operation. The governance category discusses “strategic and policy issues of cloud computing platforms” and operation category focuses “on more tactical security concern and their implementation within the architecture”.

Logical construction of security issues identified by CSA is described in Table 1:

Table 1: Security Issues identified by CSA

Strategic and Policy Issues	Tactical Issues
Governance and Enterprise Risk Management	Traditional Security, Business Continuity and Disaster Recovery
Legal Issues: Contracts and Electronic Discovery	Data Center Operations
Compliance and Audit	Incident Response, Notification and Remediation
Information Management and Data Security	Application Security
Portability and Interoperability	Encryption and Key Management
	Identity and Access Management
	Virtualization
	Security as a Service

“**Governance and Enterprise Risk Management**” focuses on agility of an organization to govern and measure risks associated with cloud computing platforms. It also recommends that security department should be included during Service Level Agreement and contractual obligations. “**Legal Issues** (Contracts and Electronic Discovery)” deals with legal issues associated with cloud computing platforms. The strategy and policy that is needed to be applied in a cloud in order to protect the information and computer systems, regulatory requirements, privacy requirements and international law to be followed by cloud providers. “**Compliance and Audit**” focuses on compliance requirements for cloud computing platforms, such as regulatory, legislative etc. and its impact on internal security policy. “**Information Management and Data Security**” focuses on data manipulation, such as creation, usage, sharing, storage, deletion, and archiving, and identifies who is responsible for data confidentiality, integrity and availability. "**Portability and Interoperability**" focuses on interoperability standards required between different cloud providers and also provides some recommendation to be followed by both deployment and delivery models of cloud computing platforms. "**Traditional Security, Business Continuity and Disaster Recovery**" focuses establishing traditional security functions, business continuity process, i.e. continuity of components of a cloud platform by assuring CIA (confidentiality, integrity, availability) and backup, disaster recovery process for cloud storage. "**Data Center Operation**" provides information on how we can evaluate the provider's data center operation in order to select the best one for long term stability. "**Incident Response Notification and Remediation**" helps us to understand complexities, brought by cloud in current incident handling program. Further, it also addresses the necessary environment that is needed to be set up between both user and provider for proper incident handling and forensic. "**Application Security**" delivers the information on modern software development cycle that is needed to be utilized by cloud computing platform. Further, it also gives us information on security threats and vulnerabilities pertaining to cloud based delivery models (IaaS, PaaS and SaaS). "**Encryption and Key Management**" gives information on protecting access to data and resources. Further, it also recommends us to use OASIS Key Management and Interoperability Protocol for key management functions. "**Identity and Access Management**" focuses on importance of identity and access management in cloud environments. Further, also focus on federated identity and the problem faced by organization while extending its identity to cloud. "**Virtualization**" discusses security issues related to system hardware and virtualization technology. Some of the items covered in this domain are hypervisor vulnerability, risk associated with multi-tenancy, VM isolation and VM co-residence. Finally, "**Security as a Service**" focuses on open issues identified by CSA which include participation of trusted third parties for security assurance, incident management, compliance attestation, and identity and access management.

Security Issues Identified by National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology is government funded organization in the US, continuously assisting cloud computing platform users by identifying security-related vulnerabilities in the platform. Security issues discussed by NIST are specifically focused to public cloud vendors, as it states that organizations have more control of each layer of security when private cloud deployment model is used. Unlike other government funded organizations like, CSA and ENISA, NIST does not make any top level classification of security issues like, organizational, policy or legal. However, each issue discussed by NIST can be linked with the sub-issue identified by other organizations. Logical construction of security issues identified by CSA is described by Table 2.

Table 2: Security Issues Identified by NIST

1.Governance
2.Compliance
3.Trust
4.Architectural
5.Identity and Access Management
6.Software Isolation
7.Data Protection
8.Availability
9.Incident Response

Governance focuses on policies and procedures needed to be followed by organizational units. It also raises an issue of information security risks. Enterprise risk is due to lack of control of services offered by cloud and it recommended using auditing tools and risking management program. "**Compliance**" discusses the issues of data location, privacy and security controls, record management, and electronic discovery. The next section "**Trust**" discusses various topic and issues of internal threats caused by multi-tenancy, maintaining data ownership and intellectual property rights, risk management, gaining visibility and security control offered by CSP. The "**Architecture**" section discusses the issues pertaining to software systems utilized by cloud platform. Most of the issues discussed in this section are due to unique characteristics of cloud computing platforms which are completely different compared to traditional data centers. The issues covered in this section are hypervisor security, virtual network protection, virtual machine images and client side protection. In "**Identity and Access Management**" the researchers from NIST focus on identityverification, authentication and access control mechanism and also recommend using SAML for authentication and XACML for access control. The next section "**Software Isolation**" warns about the threats associated with multi-tenancy such as the attack vector. "**Data Protection**" focuses on the need of data privacy and isolation, as data from different customers resides on common data center in cloud computing platforms. "**Availability**" section discusses about the threats that have a negative impact on organizational resources. Denial of service, equipment outages and natural disasters are some of the issue that is discussed. Finally, "**Incident Response**" section focus on reactive countermeasure for the attacks and threats in a cloud environment.

Security Issue Identified by European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency is another government funded organization aiming to provide better security functionality in cloud computing platform. ENISA published its first document "Cloud Computing Benefit, Risk and Recommendation for Information Security" in November 2009. The document began with highlighting key benefits of security for cloud computing platforms. The rest of the document discusses security issues which are structured into three categories. All security issues discussed in each category are listed on the table below.

Table 3: Security Issues identified by ENISA

Policy and organizational issue	**Technical issue**	**legal Issue**
Lock-in	Resource exhaustion	Subpoena and e-discovery
Loss of governance	Isolation failure	Risk from change of jurisdiction
compliance challenges	Cloud provider malicious insider	Data Protection Risk
Loss of business reputation due to tenant activities	Management Interface compromise	Licensing risk
Cloud service termination or failure	Intercepting data on transit	
Cloud provider acquisition	Data leakage on up/download, intra cloud	
	Insecure or ineffective deletion of data	
	Distributed Denial of Service	
	Economic Denial of Service	
	Loss of encryption keys	
	Undertaking malicious probes or scan	
	Compromise service engine	
	Conflict between customer hardening procedure and cloud environment	

Policy and organizational issues cover six different issues present in a cloud computing platform. Lock-in discusses about data and service portability issue in terms of adoption of cloud service model. Afterwards, loss of governance and compliance challenges are remaining in this sub domains also discuss portability issues and its impacts on organization assets, risks and vulnerabilities.

Technical issues start with a list of threats present in a computing platform. Some of the threats discussed in this topic are availability due to resource exhaustion, VM monitor vulnerability, insider threats, denial of service, network related threats, and lack of sufficient effort from consumer to secure execution environment.

Legal issues begin with subpoena and e-discovery issues, which provide information on how to respond subpoena and e-discovery issues. The rest of the legal issues discussed in this section are focused on data manipulation, data location compliance, data protection compliance and risk of losing intellectual property, when data is stored in a cloud.

IV. PROPOSED SECURITY MODEL AND IMPLEMENTATION ARCHITECTURE

We propose the frame work architecture of our central cloud security system which is designed for delivering "Security-as-a-Service" model to the cloud stack. Our central security system is based on the facts that by shifting all the security related services to application level, a generic and secure framework for cloud-based platform can be deployed. This means that all the security related services, like identity service, SSO and identity and access control, authentication and authorization mechanisms, are provided by our cloud security infrastructure.

Security System Architecture

Security system architecture is motivated by the security related services for cloud-based platform are shifted form a platform to an application level and are provided as web services by our security system architecture. One of the advantages of shifting all the security-related service to an application level is based on its design modularity and generosity. This means that our architecture is applicable to any cloud-based platform, regardless of its delivery and deployment models.

The components of our security system are based on "Service Oriented Architecture" and are responsible for managing and distributing certificates, identity management (CRUD), identity federation, creating and managing XACML-based policies, and providing strong authentication mechanisms. All the components within the system are interoperable and act as a security service providers in order to assure a secure cloud-based system. Figure 3 shows logical components of our central security system.

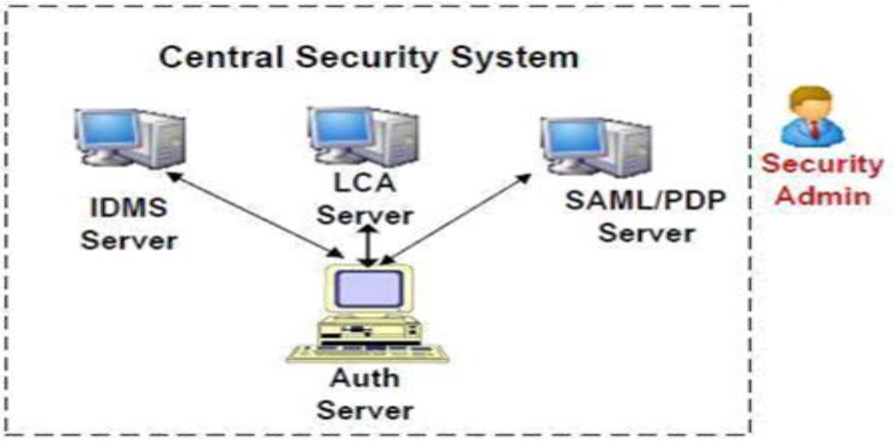


Fig 3. Central System Architecture

PKI server, also known as Local Certification Authority (LCA) in our system is responsible for issuing and distributing X509 certificates to all components in a domain. This server can either be configured as single certification authority, by generating self-signed certificates or may be linked to PKI in order to exchange certificates and establish trust relationship between various domains. In this case higher level trusted certification authority server issues certificates to the issuing CA. XACML server is also known as Policy Decision Point and is responsible for creating and validating SAML Tickets for Single Sign-On protocol. This server is also responsible for management of group, roles, XACML policy and policy sets. IDMS server is responsible for creating, reading, updating and deleting identities in a collaborative environment. Strong Authentication (SA) server performs mutual authentication with clients using various extended authentication protocols, like FIPS 196. This server also interacts with XACML policy server to generate SAML ticket for authenticated clients.

Cloud Security Infrastructure

Below Fig.4 shows logical structure of our cloud security infrastructure. The infrastructure is based on the assumption that the application service providers will focus only on their business logic rather than implementing built-in authentication and authorization services. This means that all security services are isolated and shifted towards the central security server, controlled by central security administrator. SAML and PDP system entities are responsible for delivering identity services to application service providers in both secure and interoperable manner. As shown in Figure 4 end-user (may be Enterprise Administrator) interacts with Cloud access point through Internet. The Cloud access point typically behaves as cloud entry point for our cloud security infrastructure. To have a secure communication, i.e. exchange of messages, cryptographic services like message encryption and digital signature, are required by the end-entities. This means that in order to protect the resources, the system must be facilitated with public and private key pair. Since many enterprises business, resources and applications run behind the access point in a cloud environment, access point must be preserved by some secure authentication mechanism. Implementing PKI (Public Key Infrastrucure) can fulfill our objectives.

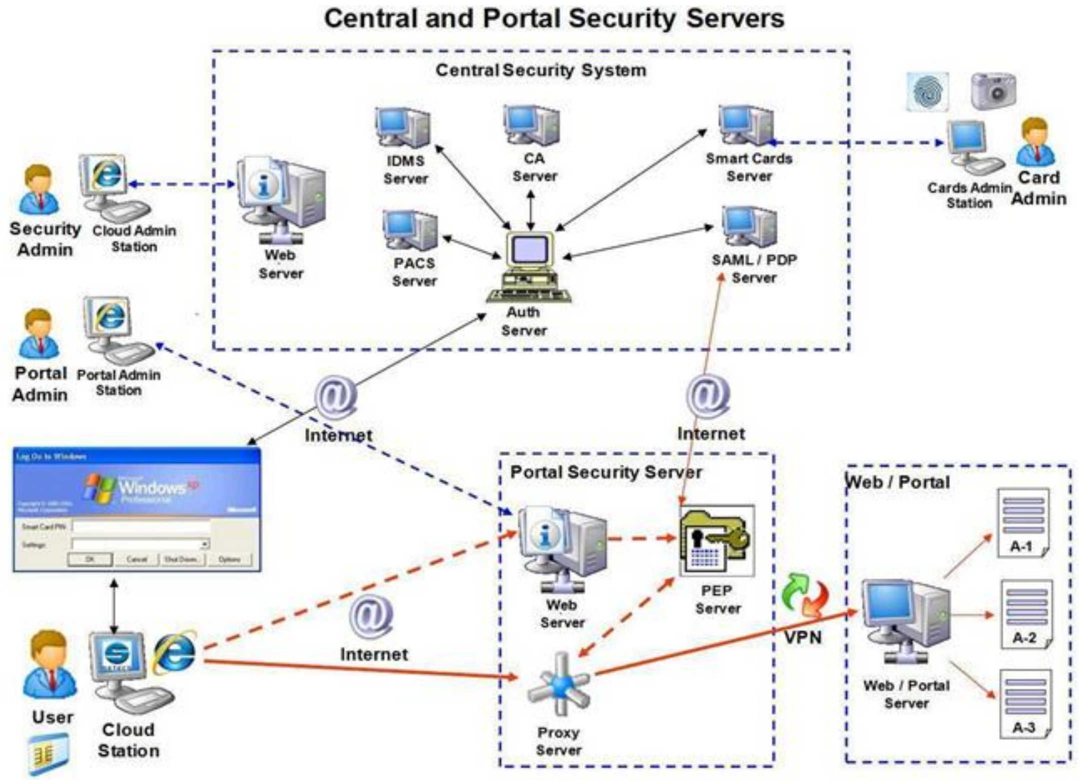


Fig.4Cloud Security Infrastructure

Security Services offered by our Central Security System

The overall approach to a design of a central security system is to provide secure means of communication for all end-users and application services running in a cloud environment. In essence, our design for providing security services is based on Service-Oriented Architecture and is defined in terms of web services. Security services offered by our central security system are authentication, authorization, identity management, access control, and SSO. Further, it is also assumed that Strong Authentication server and local certificate authority have already been designed and implemented

Single Sign-On Protocol

A single enterprise business, running in a cloud can provide more than one application to its end-users. All of the application services should authenticate clients before service transaction are executed. This means that as number of application grows, so do the number of security credentials (logins URLs, username and password). Unfortunately, having many security credentials for authentication purposes is mostly unlikely from security and system coordination and management perspective. As cloud applications are adoptable and growing in large scale, it becomes a major requirement to provide SSO service to its end-users.

The SSO service is offered by the central security server from our cloud security infrastructure. SAML server provides SSO service to application providers by providing SAML ticket which provides assurance of client identity verification for authentication purpose. Once client is authenticated, resources authorized to authenticate a client are available without the need to re-authenticate for each domain. In order to achieve the SSO service, the other components of our central security server must coordinate and interact with each other. This means that all application services and other three components of our central security system must be registered in our IDMS system in order to provide SSO service by SAML server. As shown in Figure 4, when the user wants to access resources from application service providers for the first time, the user is redirected to the central authentication server. Central authentication server, which acts as proxy server for all service providers in our central security system, is responsible for managing authentication procedure and identity verification. This means identity of the user is first verified by IDMS server and upon successful identity verification, user X.509 certificate is verified by local certification authority server. The result of this authentication procedure is then passed to the SAML server, which issues a SAML ticket based on the credential (X.509 and identity), passed to the SAML server. The SAML ticket is then passed to end-user through Authentication Server. This SAML ticket is later embedded in a request directed towards the application service providers and has a validity period. The period up-to which the SAML ticket remains validdepends on the organizational policy. A valid local session is created in order to successfully authenticate user, so that user can request services from other application service providers with the same ticket until the ticket expires. The whole mechanism is based on the assumption that there is a trust relationship between the SAML service provider and application service providers existing in different security domains.

Identity and Access Control

As mentioned earlier, cloud-based platforms are capable of hosting different application services of application service providers using the same physical resources. No matter what amount of resources application service providers are consuming for their services, each application service must be logically separated and there must be the mechanism of user provisioning, DE provisioning and overall life-cycle management of user and access in an automated fashion. One of the approaches to handle access control mechanism is to allow each application service provider to implement independently access control mechanism by means of self-governing security policies and policy enforcement points. However, the overall approach to implement independent access control and PEP seems to be fairly complex and expensive and it is not suitable for multi-domain cloud-based platform. This means that there must be an efficient way to handle identity and access control mechanisms in our cloud-based system. Moreover, with the emergence of IT in cloud-based platform, IAM in a cloud computing environment is not confined to a single domain where identity and access control mechanism of different enterprises and IT organization are needed to be considered. This means that the overall system must be architected in such a way that it must be able to provide flawless identity management, access control and identity federation. Using IAM as a web services in a Service Oriented Architecture for our cloud security infrastructure fulfills the overall requirement of identity federation and identity and access control mechanisms.

The overall approach to identity federation, based on SSO is provided by the fact that each service provider must be registered in our IDMS server. After that, based on valid credentials, each service request is processed, validated and authorized. Access control mechanism, often referred as authorization, is based on role defined by the entity of our central security system. A single Policy Decision Point (XACML) server is responsible for entire authorization process. Having a single PDP as component in our central security server optimizes the authorization process in more flexible and secure way, as it can be managed, configured administered and protected separately from application services. The PDP server supports management of groups, roles, XACML policies and policy sets defined by security administrator, based on which authorization and access control mechanism is processed. Application services are protected by PEP and can be implemented either as a separate service for each application service or integrated with application server. Figure 3 shows logical construction of the authorization process. End- user requests access to the resources, the PEP intercepts the request and creates SAML authorization request. The authorization request which contain resource, action and role of the user is then sent to the PDP Server. Based on policy and policy set, defined by security administrator, PDP server evaluates the request and sends authorization response back to the PEP. Based on the evaluation made by PDP, PEP service grants or denies the access to the requested resources.

V. CONCLUSION

Design and implementation of a generic and secure architecture for cloud computing platform is still an open issue in the field of security for IT organizations. Due to the varying nature of computing platform, in terms of delivery and deployment models, cloud still needs generic and secure architecture in term of its adoption. We focused on design and implementation of a generic and secure architecture for cloud computing platforms. The whole architecture is based on the concept of Service-Oriented Architecture that can be deployed on any computing platform, regardless of its deployment and delivery model. Based on our prototype implementation during our research we were able to conclude that by shifting all of the security services to application level, a secure computing platform can provide services like Single Sign-On, Identity and Access Management and certificate-based authentication. Moreover, all security related services, offered by our central security system, are delivered in terms of web services, thereby, they possess significant advantage in terms of their usability, deploy ability, interoperability, and scalability for any computing platform.

REFERENCES

[1]. Wayne Jansen, Timothy Grance (2011) “Guidelines in security and privacy in cloud computing” National institute of standards and technology U.S department of commerce, NIST special publication 800-144.

[2]. YashpalKadam(2011) “Security issues in cloud computing- A transparent view” Int. J Comp Sci. Emerging Tech, Vol- 2 No 5 October, 2011.

[3]. Kevin Hamlen, The University of Texas at Dallas, USA (2010) “Security issues in cloud computing” International Journal of Information Security and Privacy, 4(2), 39-51.

[4]. Volker Fusenig and Ayush Sharma (2012) “Security Architecture for Cloud Networking” International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium 978-1-4673-0009-4/12.

[5]. Paul Simmonds, Chris Rezik, Arhie Reed [2011] “Security Guidance for Critical Areas of Focus in Cloud Computing v.3.0.”CSA publication 2011.

[6]. Jianyong Chen, Yang Wang, and Xiaomin Wang (2012) "On-Demand Security Architecture for Cloud Computing" IEEE Computer Society, 0018-9162/12.

[7]. Kandukuri BR, Paturi VR, Rakshit A. "Cloud security issues". In: IEEE international conference on services computing, 2009, p. 517–20.

[8]. Kaufman LM. "Data security in the world of cloud computing, security and privacy" IEEE 2009; 7(4):61–4.

[9]. Z. Xiao andY.Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp.843–859, 2013.

[10]. N. Kshetri, "Privacy and security issues in cloud computing: the role of institutions and institutional evolution," Telecommunications Policy, vol. 37, no. 4-5, pp. 372–386, 2013.

[11]. Sosinsky B, Cloud Computing Bible. 1st ed. Wiley; 2011.

[12]. Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud." Internet Computing, IEEE 16.1 (2012): 69-73.

[13]. Okuhara, Masayuki, Tetsuo Shiozaki, and Takuya Suzuki. "Security Architecture for Cloud Computing." FUJITSU Sci. Tech. J 46.4 (2010): 397-402.

[14]. ENISA – Cloud Computing Security Strategy, Dr Giles Hogben, www.enisa.europa.eu

[15]. K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.

[16]. C. Cachin and M. Schunter, "A cloud you can trust," IEEESpectrum, vol. 48, no. 12, pp. 28–51, 2011.

[17]. Cloud Single Sign-on and Authorization Services, Davit Hakobyan, Degree project in Second cycle, Stockholm, Sweden 2012, KTH (Royal Institute of Technology)

[18]. Cong Wang, Qian Wang and KuiRen,"Ensuring Data Storage Security in Cloud computing"978-1- 4244 -3876-1/2009 IEEE.

[19]. John Harauz, Lori M. Kaufman, Bruce Potter, "Data security in the world of cloud computing", 2009 IEEE CO Published by the IEEE Computer and Reliability Societies.

[20]. Guidelines for Managing Security and Privacy (NIST Special Publication 800-144), January 24, 2012

AUTHOR PROFILE

VenkateswarluManintireceived Master's Degree from Jawaharlal Nehru University, Anantapur, AP. and pursuing Ph.D. from MJPRU, UP. Hisresearch interest in Cloud Security Mechanism's, in Cloud computing storage.

Dr. P. Nageshwar, M.C.A., Ph.D. Working as a Asst. Professor, Department of Computer Applications, M.V.S Govt. Degree College, Mahabubnagar-Telanganga State-India. His research interest in Cloud Security Mechanism's, in cloud computing storage.